Practical Integration of Quantum Key Distribution with Next-Generation Networks

A. B. Price, A. Aguado, E. Hugues-Salas,
P. A . Haigh, P. Sibson, J. Marhuenda,
J. Kennard, J. G. Rarity, M. G. Thompson,
R. Nejabati, D. Simeonidou and C. Erven

University of BRISTOL
QUANTUM COMMUNICATIONS HUB
EPSRC
Pioneering research and skills

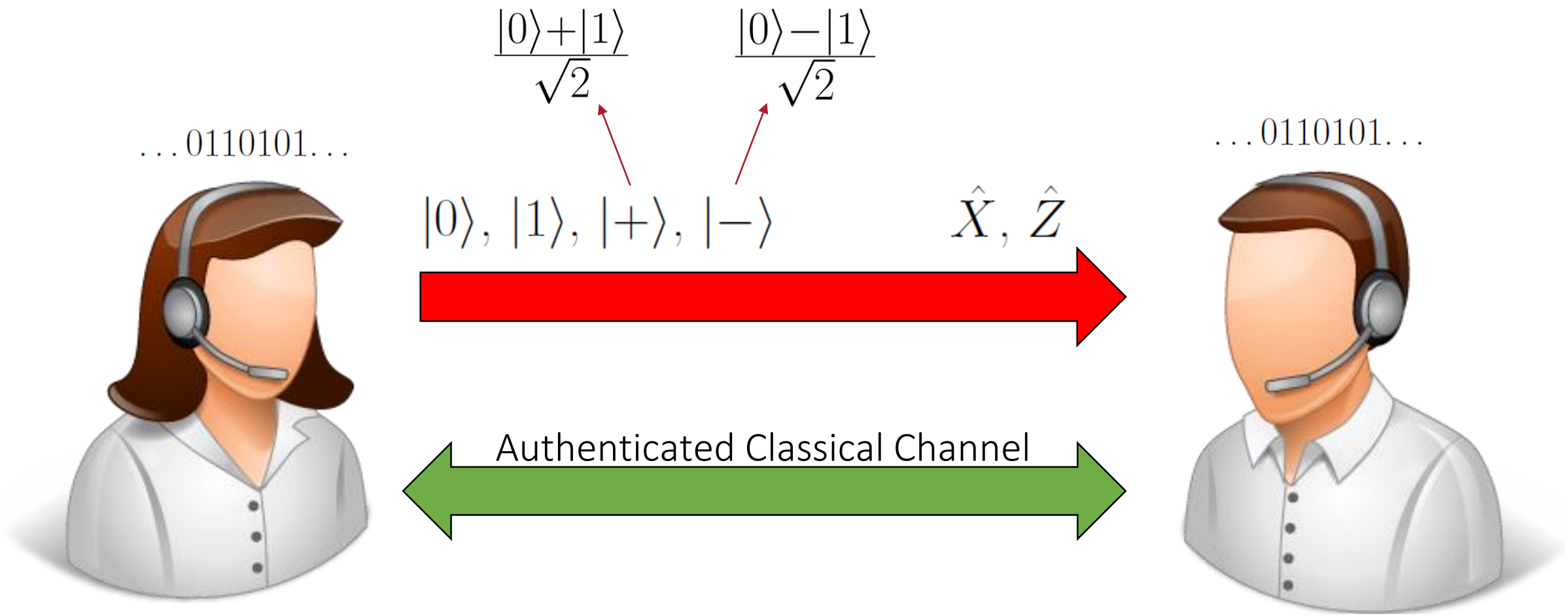
Overview

- QKD Refresher
- Networks of the Future
- Emulating a Software Defined Network
- Time-Sharing QKD Systems
- Distributing Virtual Network Functions
- Next steps

QKD Refresher

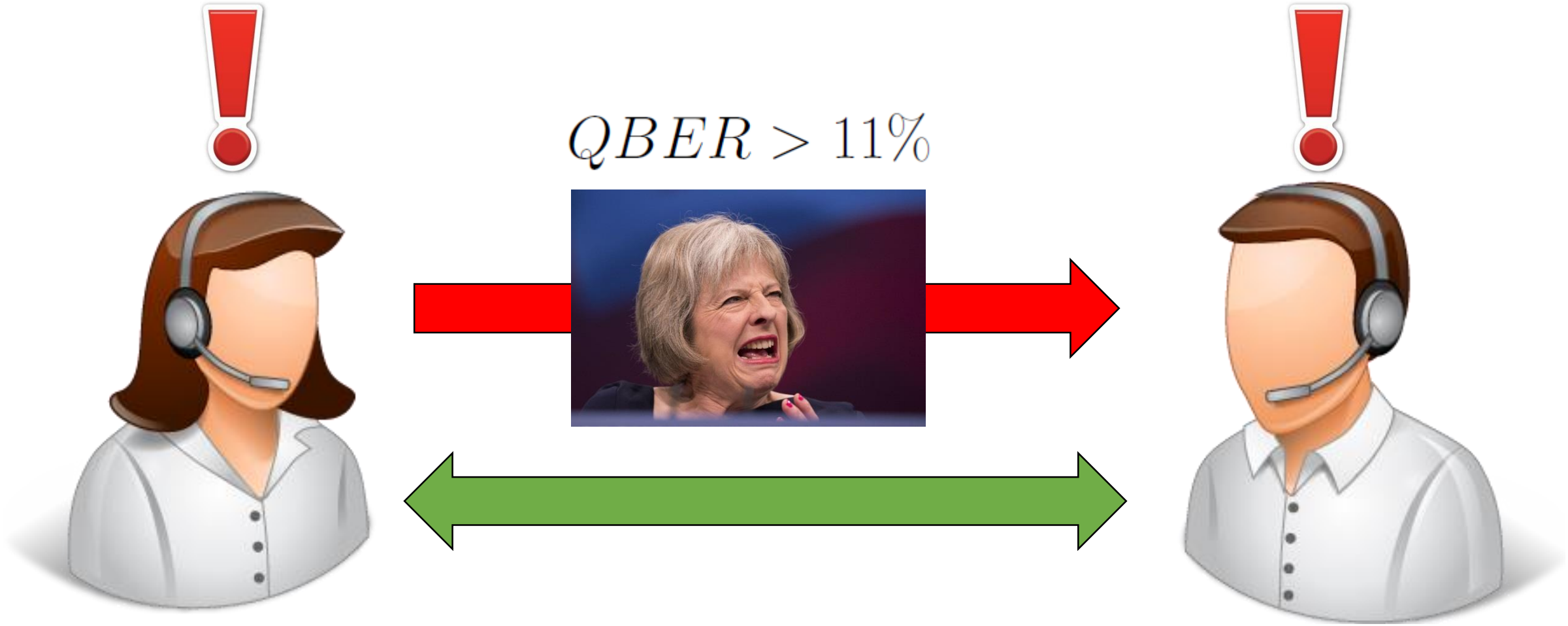
- Shor’s algorithm can be used to attack conventional key distribution methods.
- Grover’s search strengthens brute force attacks.
- Need a quantum-secure method of key distribution to use alongside conventional ciphers reinforced against Grover’s.

QKD Refresher



C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing **175** (1984).
V. Scarani, A. Acin, G. Ribordy and N. Gisin, *Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations*, Phys. Rev, Lett. **92** (2004).

QKD Refresher



C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing **175** (1984).
V. Scarani, A. Acin, G. Ribordy and N. Gisin, *Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations*, Phys. Rev, Lett. **92** (2004).

QKD Refresher

One Time Pad

Mathematically secure

Infeasible for day-to-day communications

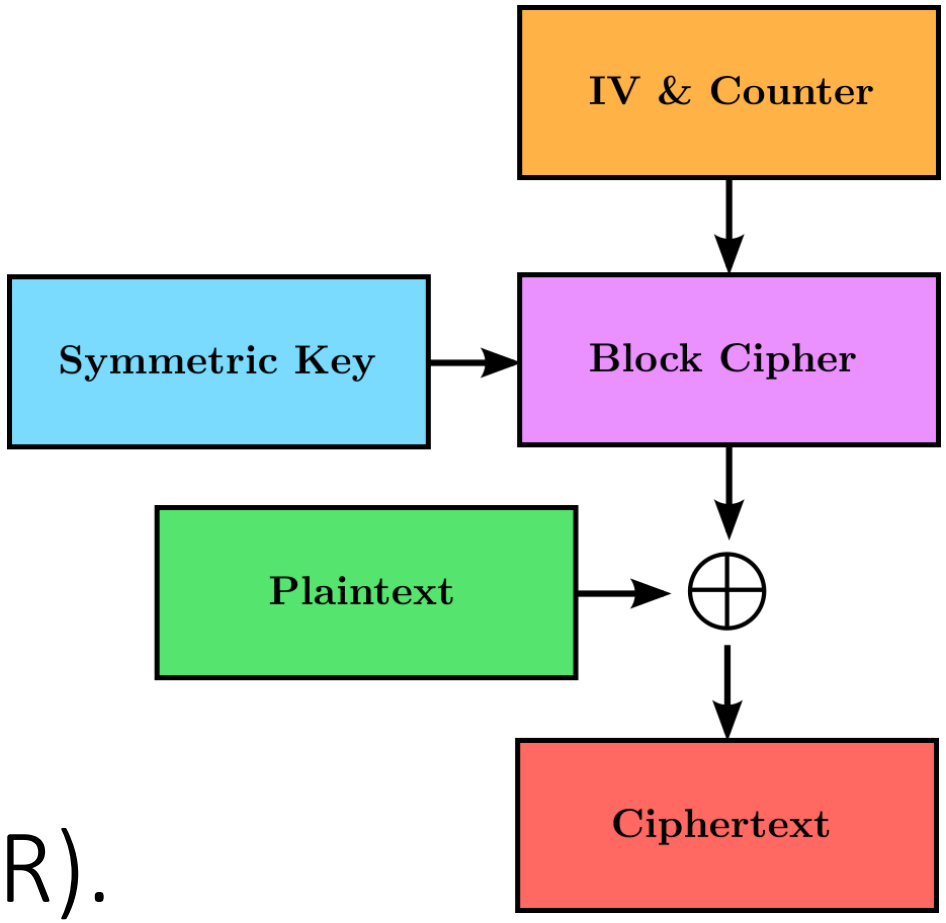
AES

Secure enough

Widely used in day-to-day communications

AES

Enciphers and deciphers messages in 128-bit blocks with **256-bit** keys for post-quantum security. Can perform full encryption when operating in the correct mode (e.g. CTR).



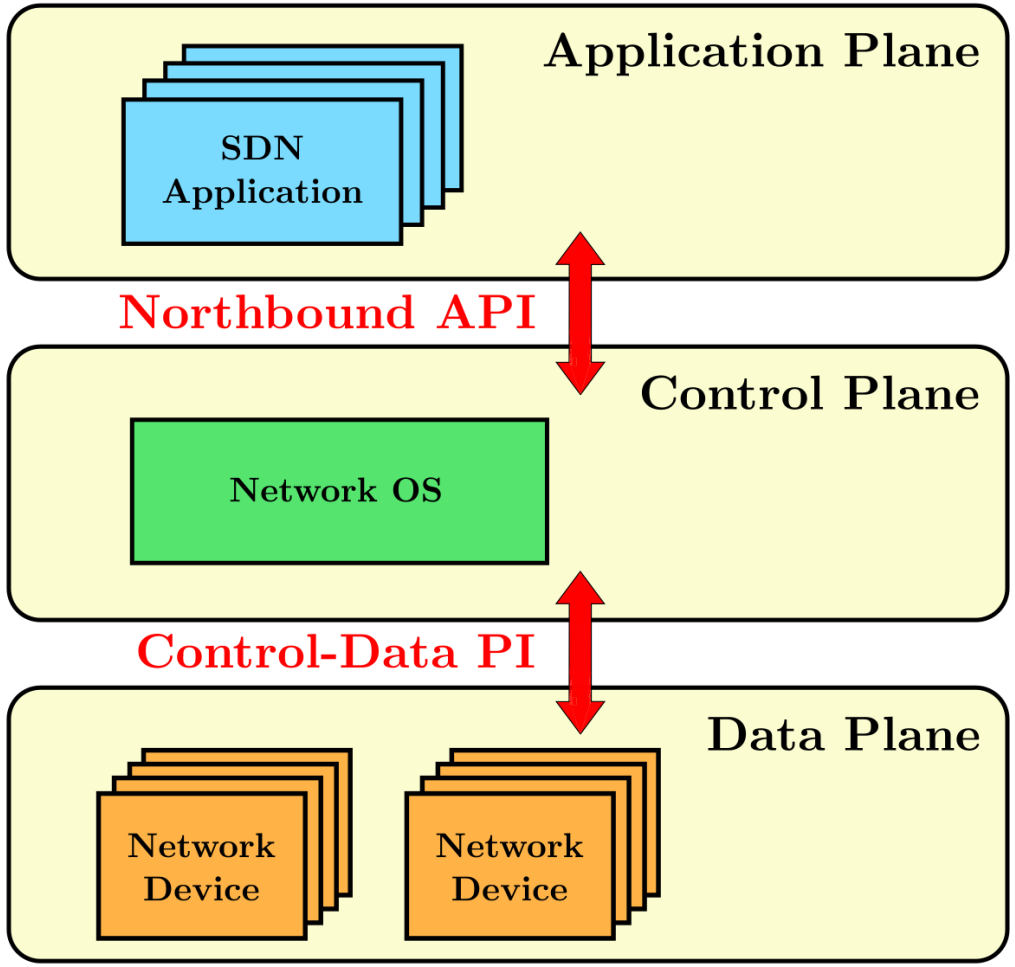
M. Dworkin, *Recommendation for Block Cipher Modes of Encryption: Methods and Techniques*, NIST 800-38A (2001).

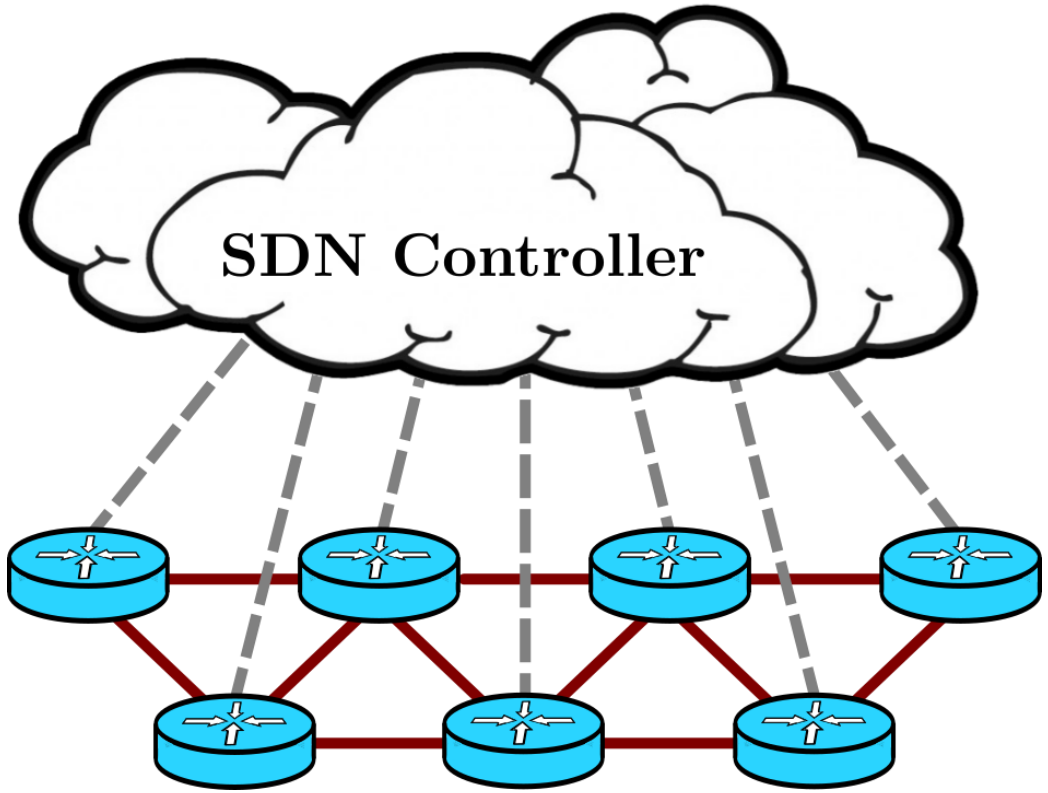
Networks of the Future

Future networks will be software-defined, deploying data handling rules as software rather than hardcoding them in the firmware of devices, allowing global reconfigurability of the network from a single location as and when required.

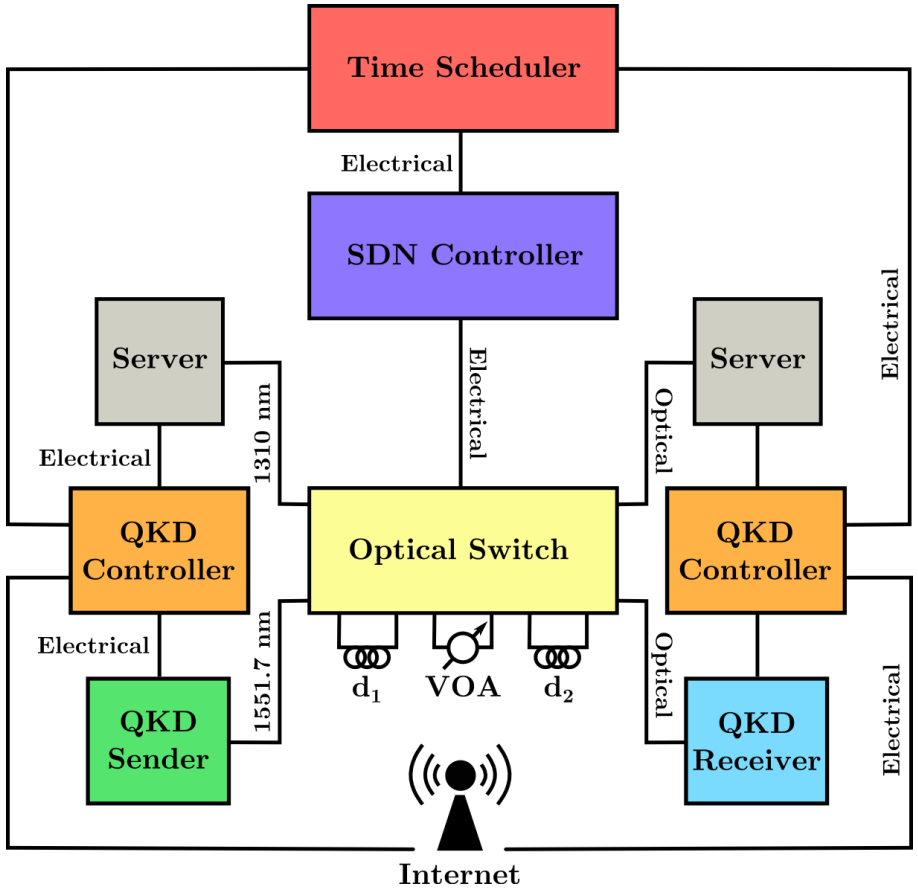
F. Hu, Q. Hao and K. Bao, *A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation*, IEEE Communications Surveys and Tutorials **16** (2014).

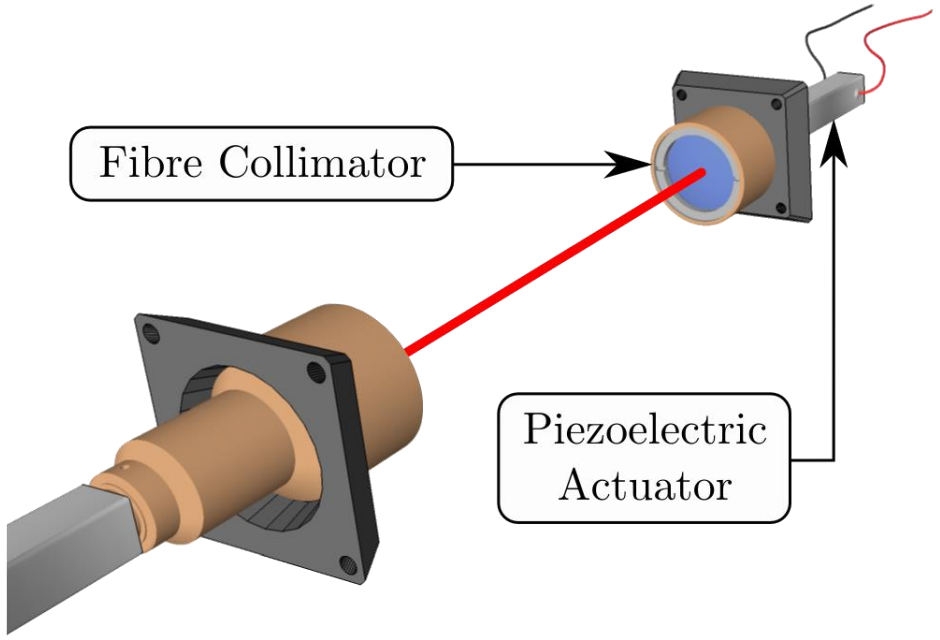
Networks of the Future



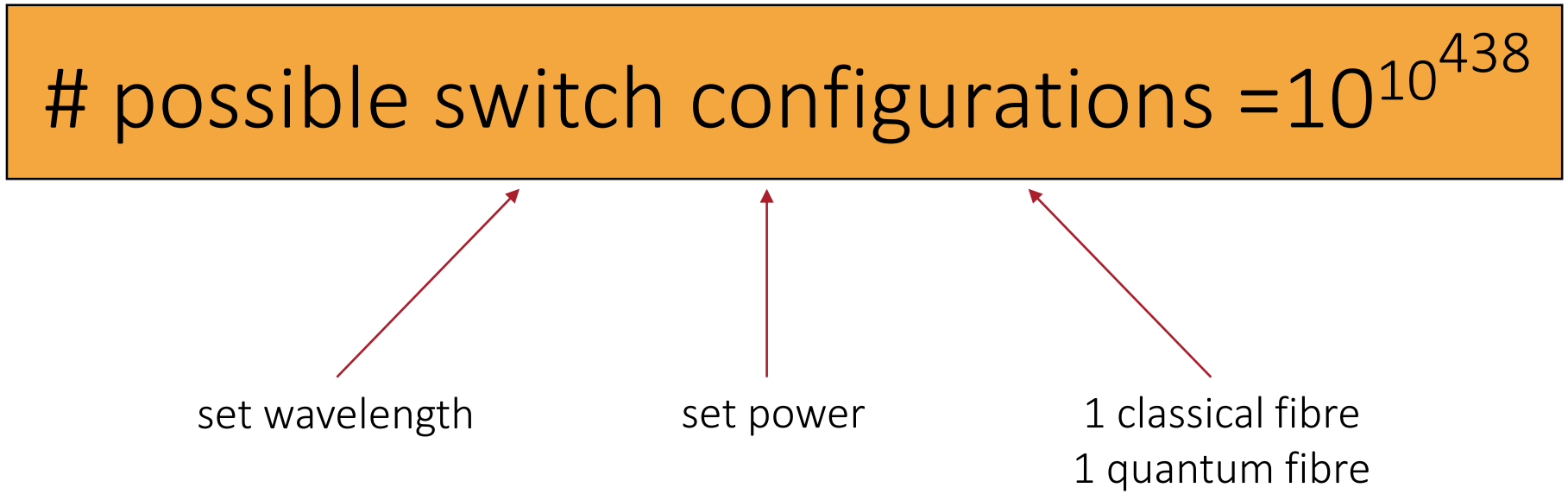


Emulating a Software Defined Network





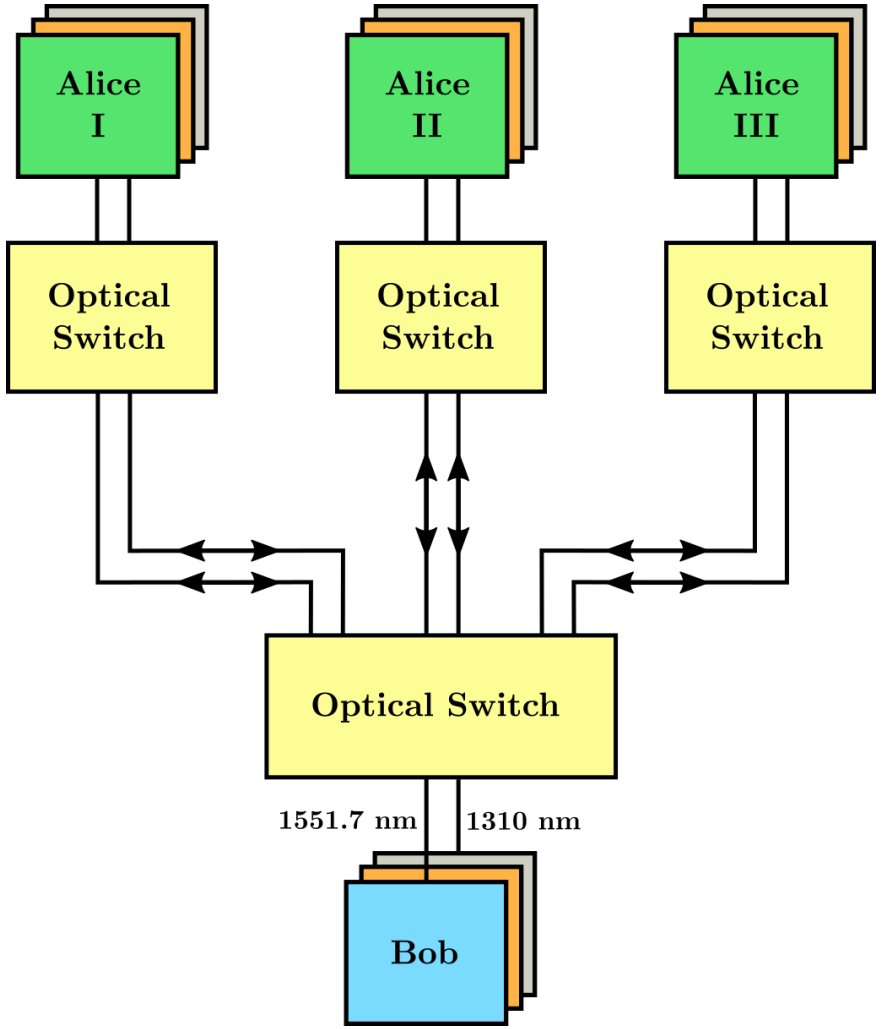
Emulating a Software Defined Network

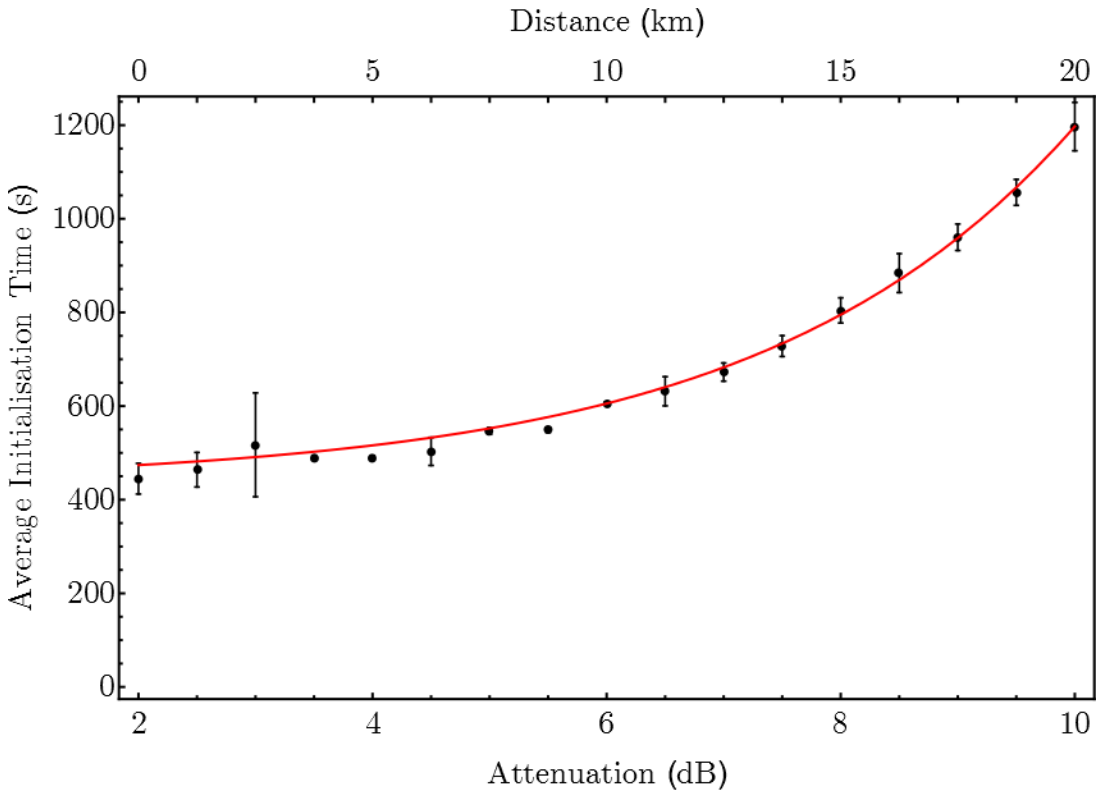


Best case: Negligible cross-talk

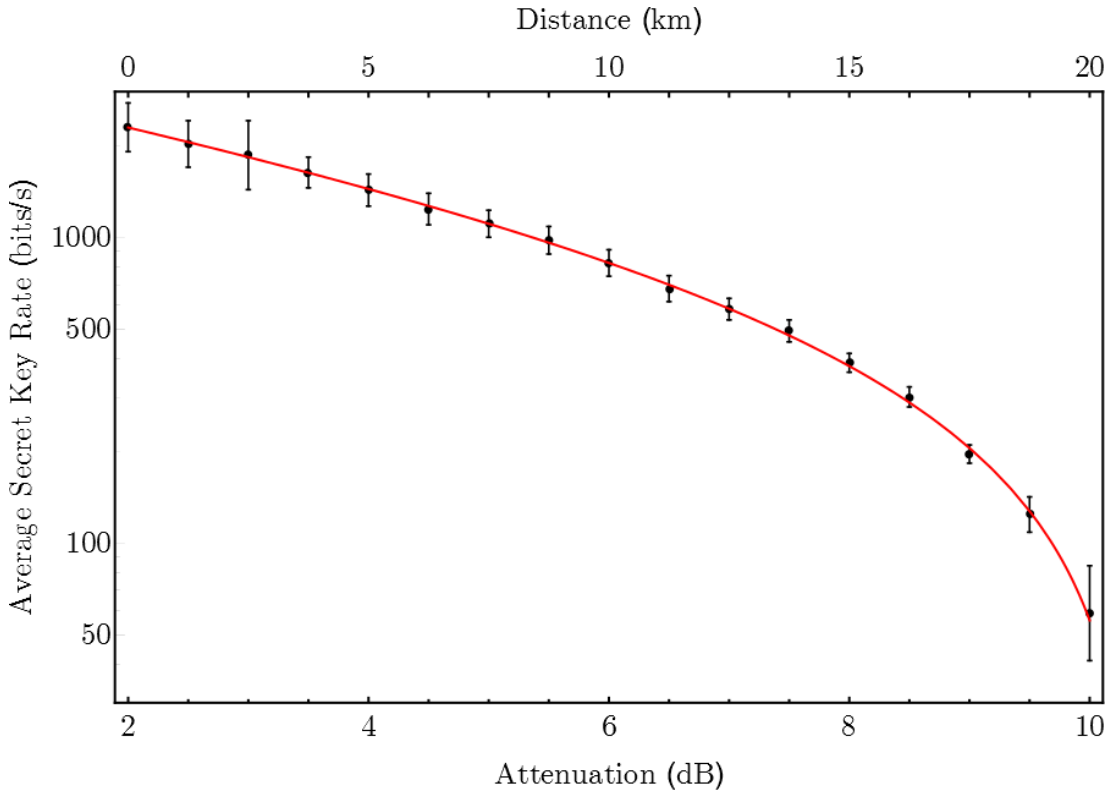
Worst case: 49.1 x 10^3 counts/s

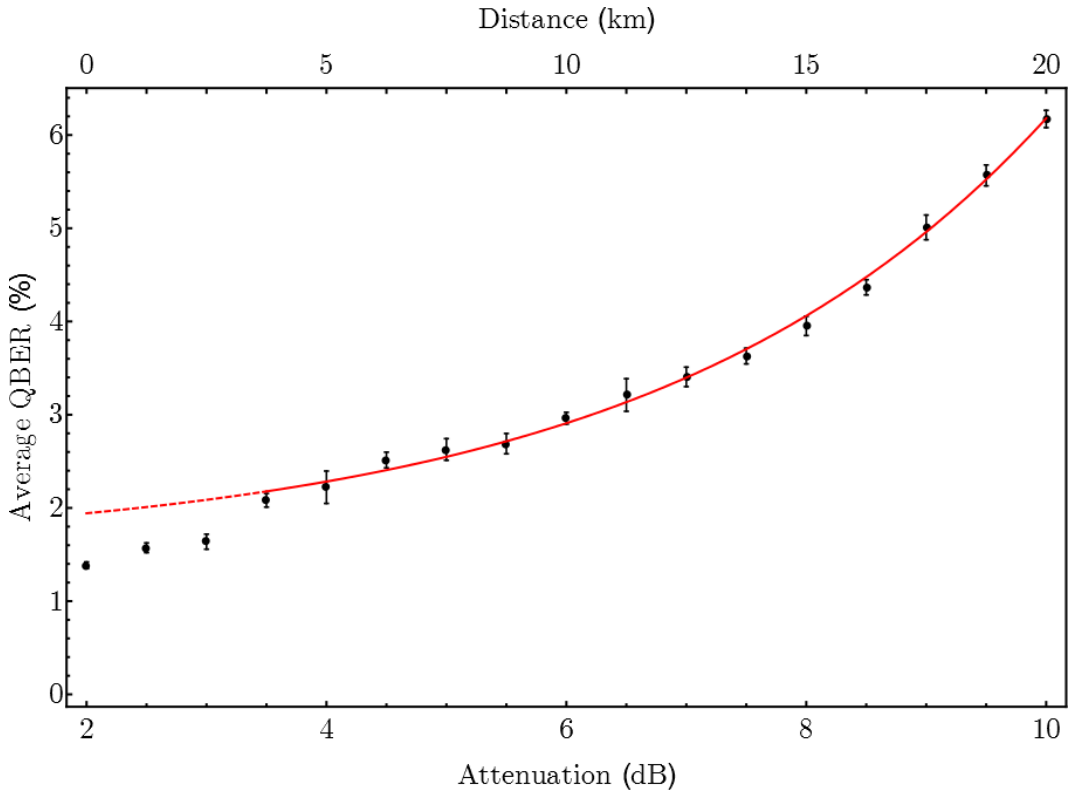
Time-Sharing QKD Systems





Distributing Virtual Network Functions





10 km data centre: Secret key rate = 825 bits/s, QBER = 2.96 %

Distributing Virtual Network Functions

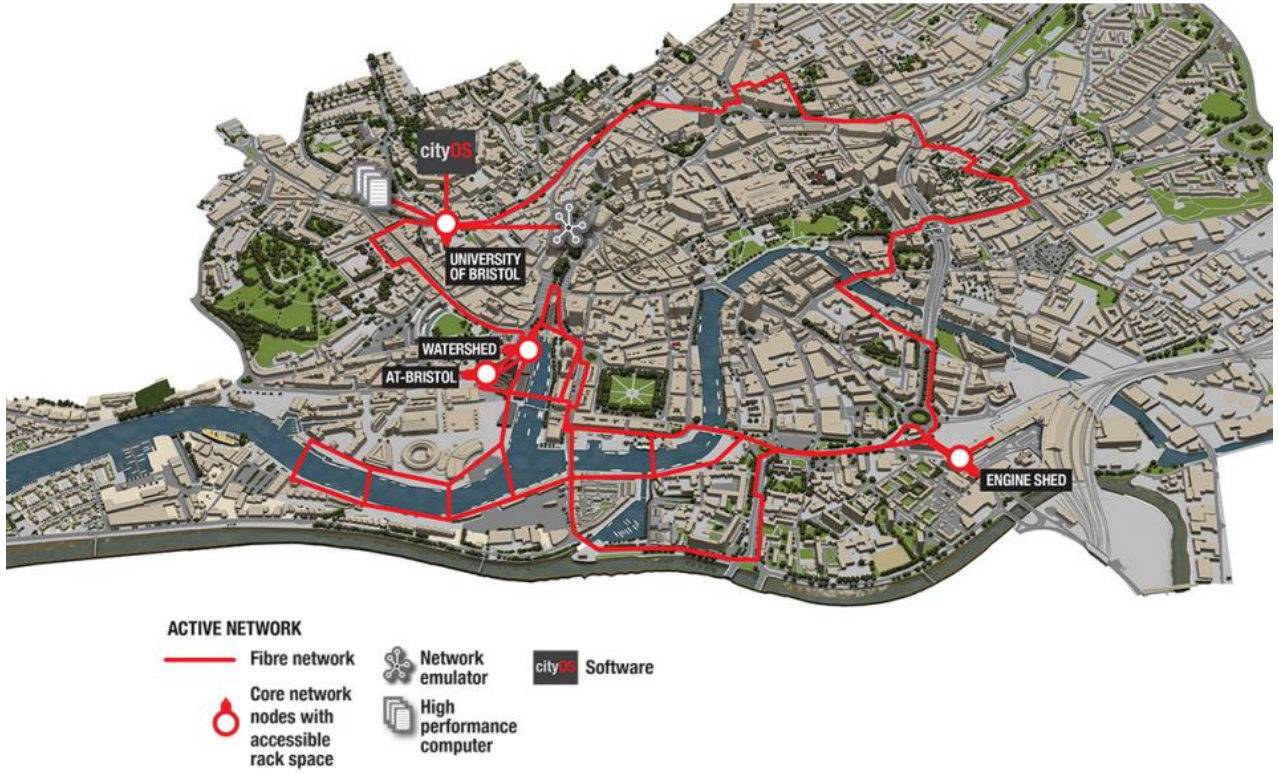
- Transmitted AES-encrypted Windows VM (**14.831 GiB**), Ubuntu VM (**0.178 GiB**) and CentOS OVS_LC (**0.716 GiB**).
- AES GCM encrypts **≤ 64 GiB** per key/IV pair.
- **606 ± 2 s** to generate each **223 ± 1 kbit** set of VNF keys allows **79** Alices per Bob in 10G networks.

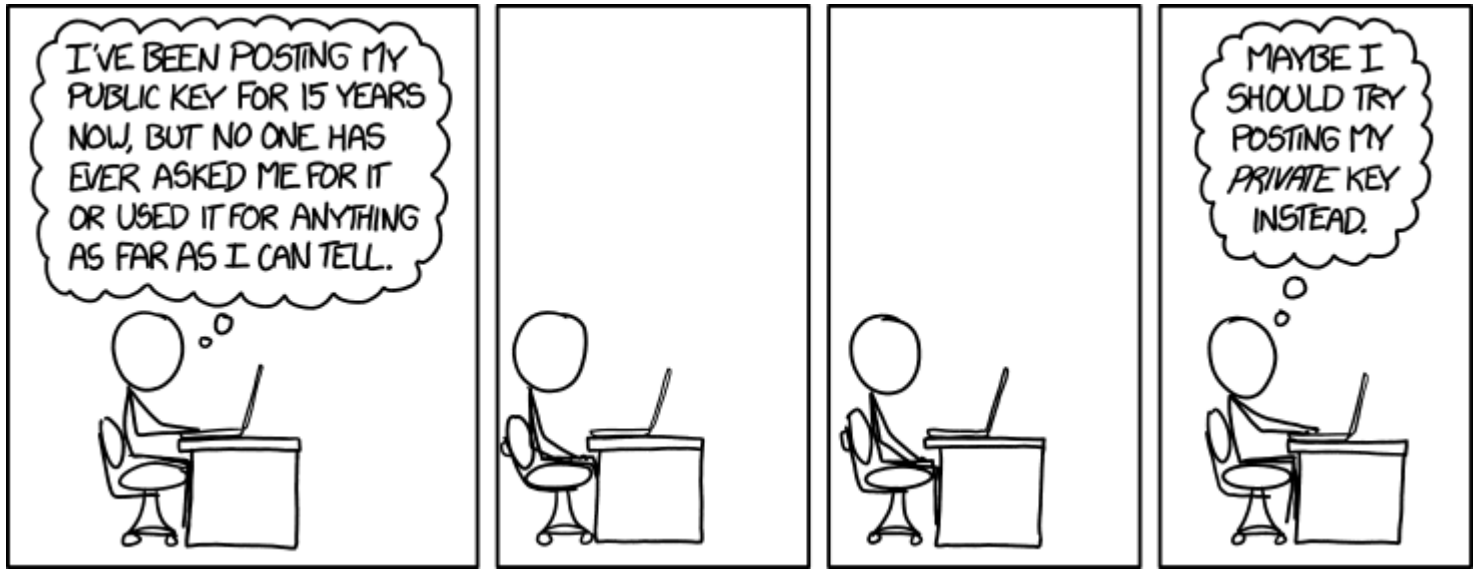
Summary and Next Steps

- Demonstrated compatibility of QKD with the software defined networking paradigm.
- Utilised the SDN framework to time-share commercial QKD systems.
- Secured the transfer of virtual network functions using quantum keys.

Summary and Next Steps

The Bristol is Open metropolitan-scale SDN relies on VNF distribution to maintain a versatile infrastructure.





https://xkcd.com/1553/